# WAS Scan Report

Qualys. Express

## Scan Report

28 Jul 2025

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Tibu Padmakumar
craka8tp

Cirakas Consulting Private Ltd

null, None null
India

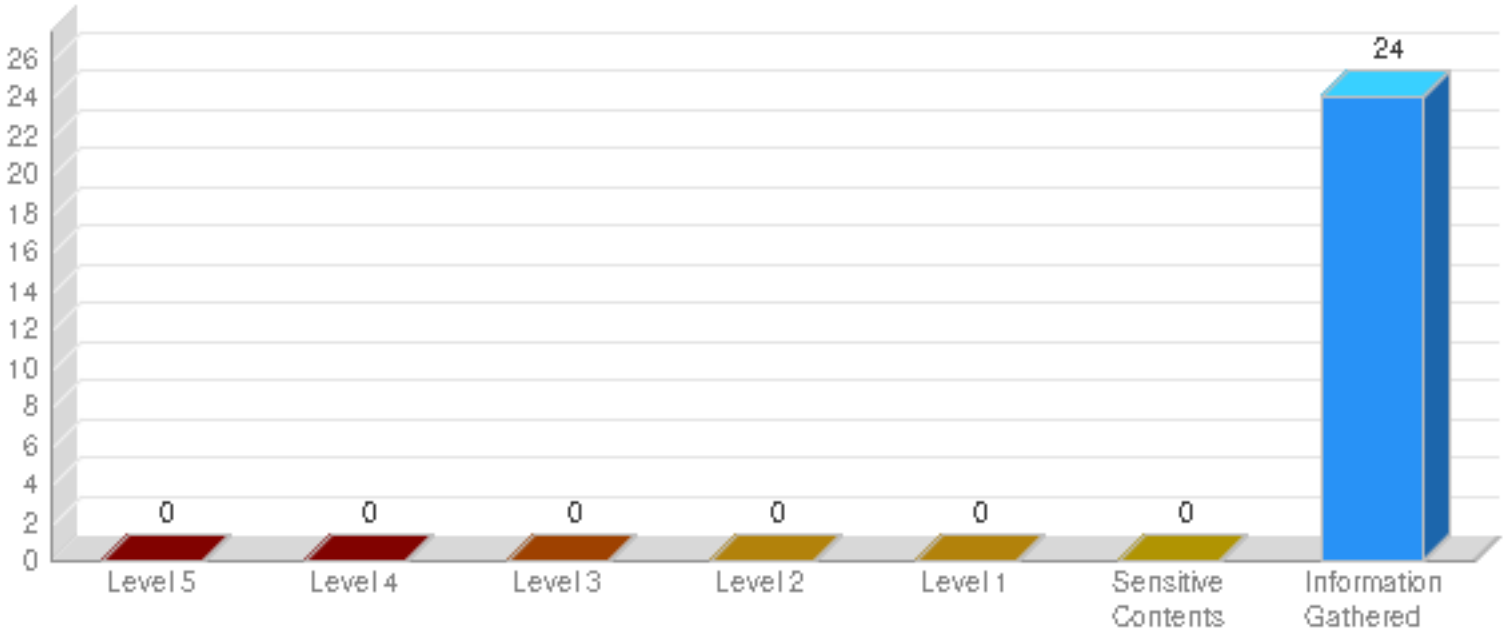
## Target and Filters

| | |
|---|---|
| Scans (1) | Jul 28, 2025 |
| Web Applications (1) | DictateMed API 2 |

## Summary

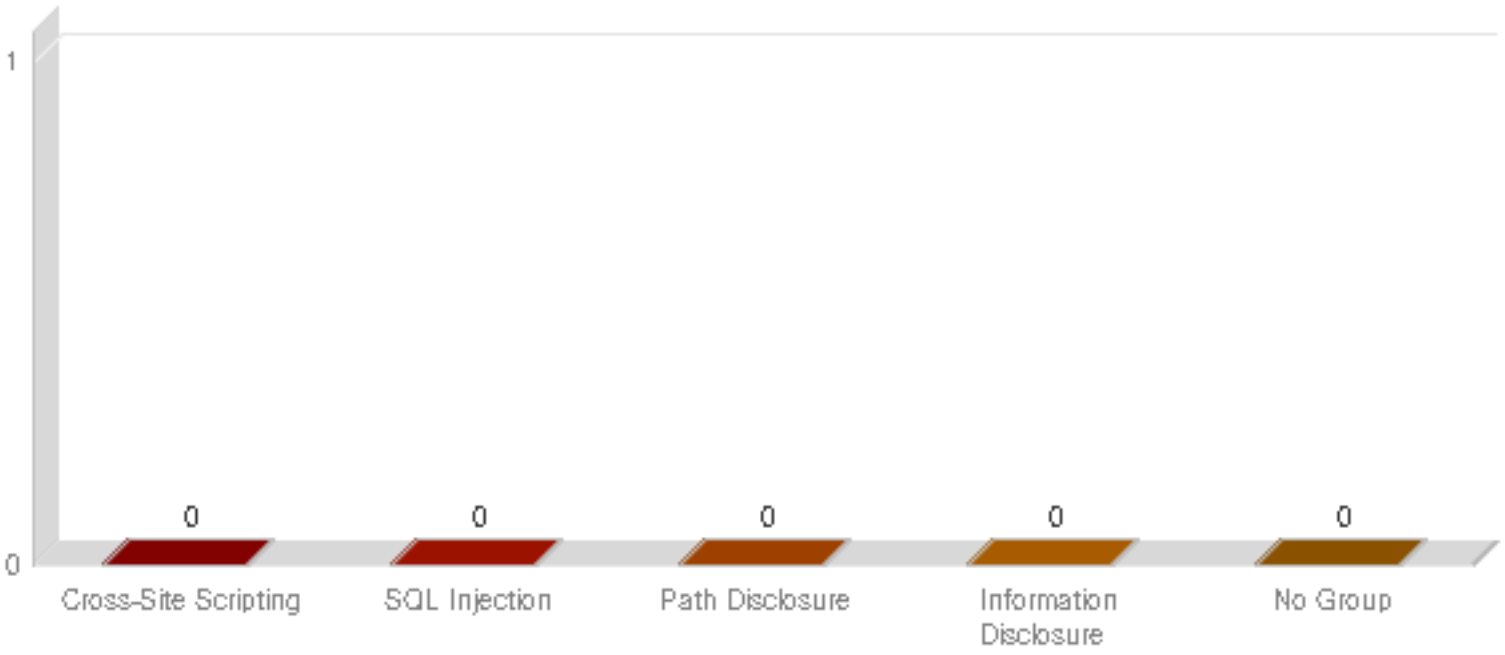
| Security Risk | Vulnerabilities | Sensitive Contents | Information Gathered |
|---|---|---|---|
| - | 0 | 0 | 24 |

### Findings by Severity

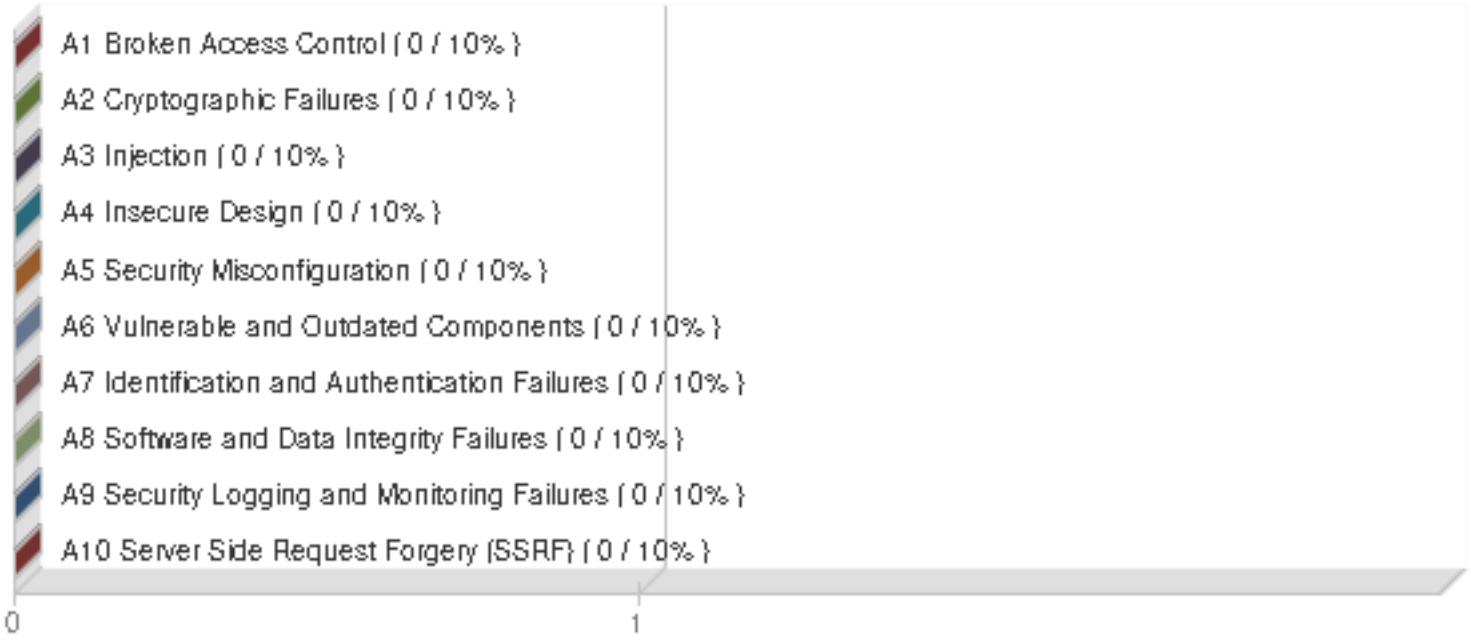


# WAS Scan Report

## Vulnerabilities by Group




## OWASP Top 10 2021 Vulnerabilities




| Scan | Date | Level 5 | Level 4 | Level 3 | Level 2 | Level 1 | Sensitive Contents | Information Gathered |
|---|---|---|---|---|---|---|---|---|
| Jul 28, 2025 | 28 Jul 2025 13:54 GMT +0630 | 0 | 0 | 0 | 0 | 0 | 0 | 24 |

# WAS Scan Report

## Results(24)

### Information Gathered (24)

#### Scan Diagnostics (19)

##### 150042 Server Returns HTTP 5XX Error Code During Scanning (1)

150042 Server Returns HTTP 5XX Error Code During Scanning

| | | | |
|---|---|---|---|
| Finding # | **4549109**(129546116) | Severity | Information Gathered - Level 3 |
| Unique # | **85e2c3ea-a337-4949-aa78-934ead579ba0** | | |
| Group | Scan Diagnostics | Detection Date | 28 Jul 2025 13:54 GMT+0630 |
| CWE | CWE-209, CWE-550 | | |
| OWASP | A5 Security Misconfiguration | | |
| WASC | WASC-14 SERVER MISCONFIGURATION | | |

Details

**Threat**

During the WAS scan, links or end points with HTTP 5xx response code were observed and these are listed in the Results section. The HTTP 5xx message indicates a server error. The list of supported 5xx response code are as below:

500 - Internal Server Error
501 - Not Implemented
502 - Bad Gateway
503 - Service Unavailable
504 - Gateway Timeout
505 - HTTP Version Not Supported

**Impact**

The presence of a HTTP 5xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities. If expected response is not received then vulnerabilities present on such links or end points may not be detected.

**Solution**

Review each link to determine why the server encountered an error when responding to the link. Review and investigate the results of QID 150528 which lists 4xx errors and QID 150019 which lists unexpected response codes.

Results

https://api.dictatemed.com/api/v1/dictations/update/dictation
https://api.dictatemed.com/api/v1/auth/verify/email
https://api.dictatemed.com/api/v1/auth/signup
https://api.dictatemed.com/api/v1/auth/signin
https://api.dictatemed.com/api/v1/auth/reset-password
https://api.dictatemed.com/api/v1/auth/refresh-token
https://api.dictatemed.com/api/v1/auth/forgot-password
https://api.dictatemed.com/api/v1/auth/change-password

##### 6 DNS Host Name (1)

# WAS Scan Report

## 6 DNS Host Name

| | | | |
|---|---|---|---|
| **Finding #** | **4549112**(129546119) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **e7abb779-a187-416a-9e98-b6a045c41340** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

**Impact**
N/A

**Solution**
N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | - |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | - |
| **Result** | #table IP_address Host_name 13.53.167.226 api.dictatemed.com 13.53.167.226 ec2-13-53-167-226.eu-north-1.compute.amazonaws.com |

### Info List

**Info #1**

**38116 SSL Server Information Retrieval** (1)

# WAS Scan Report

## 38116 SSL Server Information Retrieval

| | | | |
|---|---|---|---|
| **Finding #** | **4549118**(129546125) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **4ab01b17-f803-41b3-95e5-4b65147f653b** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

#### Threat

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

#### Impact

N/A

#### Solution

N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | 443 |
| **Result** | #table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.2_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.3_PROTOCOL_IS_ENABLED _ _ _ _ _ TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(1 MEDIUM TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/ POLY1305(256) HIGH TLS13-AES-128-CCM-SHA256 N/A N/A AEAD AESCCM(128) MEDIUM |

## Info List

### Info #1

### Ciphers

| Name | Auth | Encryption | Grade | Key Exchange | Mac | Protocol |
|---|---|---|---|---|---|---|
| TLS13-AES-128-GCM-SHA256 | N/A | AESGCM(128) | MEDIUM | N/A | AEAD | TLSv1.3 |
| TLS13-AES-256-GCM-SHA384 | N/A | AESGCM(256) | HIGH | N/A | AEAD | TLSv1.3 |
| TLS13-CHACHA20-POLY1305-SHA256 | N/A | CHACHA20/POLY1305(256) | HIGH | N/A | AEAD | TLSv1.3 |
| TLS13-AES-128-CCM-SHA256 | N/A | AESCCM(128) | MEDIUM | N/A | AEAD | TLSv1.3 |

**38291 SSL Session Caching Information** (1)

# WAS Scan Report

## 38291 SSL Session Caching Information

| | | | |
|---|---|---|---|
| **Finding #** | **4549116**(129546123) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **b1be1d20-7cb2-418f-8b8b-d625cc4d6150** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

#### Threat

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

#### Impact

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

#### Solution

N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | 443 |
| **Result** | TLSv1.3 session caching is enabled on the target. |

### Info List

**Info #1**

**38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance** (1)

# WAS Scan Report

## 38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

| | | | |
|---|---|---|---|
| **Finding #** | **4549117**(129546124) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **3383eed8-e17a-4259-a159-256a6e76f718** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

**Impact**

N/A

**Solution**

N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | 443 |
| **Result** | #table cols=2 my_version target_version 0304 rejected 0399 rejected 0400 rejected 0499 rejected |

### Info List

**Info #1**

**38600 SSL Certificate will expire within next six months** (1)

# WAS Scan Report

## 38600 SSL Certificate will expire within next six months

| | | | |
|---|---|---|---|
| **Finding #** | **4549114**(129546121) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **819d1963-06a6-4840-9b11-343414c3003c** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

**Impact**

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

**Solution**

Contact the certificate authority that signed your certificate to arrange for a renewal.

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | 443 |
| **Result** | Certificate #0 CN=api.dictatemed.com The certificate will expire within six months: Sep 22 13:03:52 2025 GMT |

### Info List

**Info #1**

Certificate Fingerprint:3A0CD0954072E8912F11B52078E0E0A4E36423FA653D66B768E697402B65E77F

## 38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (1)

# WAS Scan Report

## 38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

| | | | |
|---|---|---|---|
| **Finding #** | **4549119**(129546126) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **0a628be7-7104-4f57-a03b-b669e9aaa534** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

**Impact**

N/A

**Solution**

N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | 443 |
| **Result** | #table cols="6" NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.3 _ _ _ _ _ DHE ffdhe2048 2048 110 low DHE ffdhe3072 3072 yes 132 low DHE ffdhe4096 4096 yes 150 low DHE ffdhe6144 6144 yes 178 low DHE ffdhe8192 8192 yes 202 low ECDHE x2 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes 260 low ECDHE secp384r1 384 yes 192 lo |

## Info List

### Info #1

#### Kexs

| Kex | Group | Protocol | Key Size | Fwd Sec | Classical | Quantam |
|---|---|---|---|---|---|---|
| DHE | | TLSv1.3 | 2048 | yes | 110 | low |
| DHE | | TLSv1.3 | 3072 | yes | 132 | low |
| DHE | | TLSv1.3 | 4096 | yes | 150 | low |
| DHE | | TLSv1.3 | 6144 | yes | 178 | low |
| DHE | | TLSv1.3 | 8192 | yes | 202 | low |
| ECDHE | | TLSv1.3 | 256 | yes | 128 | low |
| ECDHE | | TLSv1.3 | 256 | yes | 128 | low |
| ECDHE | | TLSv1.3 | 448 | yes | 224 | low |
| ECDHE | | TLSv1.3 | 521 | yes | 260 | low |
| ECDHE | | TLSv1.3 | 384 | yes | 192 | low |

**38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties** (1)

# WAS Scan Report

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

| | | | |
|---|---|---|---|
| **Finding #** | **4549120**(129546127) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **2ced9fac-a4ab-467a-a7b1-99201ba4e7c5** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat

The following is a list of detected SSL/TLS protocol properties.

### Impact

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

### Solution

N/A

## SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | 443 |
| **Result** | #table cols="2" NAME STATUS TLSv1.3 _ Heartbeat no Cipher_priority_controlled_by client OCSP_stapling no SCT_extension no |

## Info List

### Info #1

#### Props

| Name | Value | Protocol |
|---|---|---|
| Heartbeat | no | TLSv1.3 |
| Cipher priority controlled by | client | TLSv1.3 |
| OCSP stapling | no | TLSv1.3 |
| SCT extension | no | TLSv1.3 |

**38718 Secure Sockets Layer (SSL) Certificate Transparency Information** (1)

# WAS Scan Report

## 38718 Secure Sockets Layer (SSL) Certificate Transparency Information

| | | | |
|---|---|---|---|
| **Finding #** | **4549115**(129546122) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **6cfd9610-4efe-4164-87a5-02381aae3be1** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

**Impact**
N/A

**Solution**
N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | 443 |
| **Result** | #table cols="6" Source Validated Name URL ID Time Certificate_#0 _ CN=api.dictatemed.com _ _ _ Certificate no (unknown) (unknown) a442c506496061548f0fd4ea9cfb7a2d26454d87a97f2fdf4559f6274f3a8454 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) ccfb0f6a85710965fe959b53cee9b27c22e9855c0d978db6a97e54c0fe4c0db0 Thu_01_Jan_1970_12:00:00_AM_GMT |

### Info List

**Info #1**

Certificate Fingerprint:3A0CD0954072E8912F11B52078E0E0A4E36423FA653D66B768E697402B65E77F

## 45038 Host Scan Time - Scanner (1)

# WAS Scan Report

## 45038 Host Scan Time - Scanner

| | | | |
|---|---|---|---|
| **Finding #** | **4549121**(129546128) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **6cc0a62f-341a-4641-b306-6df8940743a3** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

**Impact**

N/A

**Solution**

N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | - |
| **Virtual Host** | api.dictatemed.com |
| **IP** | 13.53.167.226 |
| **Port** | - |
| **Result** | Scan duration: 1251 seconds Start time: Mon Jul 28 08:23:45 UTC 2025 End time: Mon Jul 28 08:44:36 UTC 2025 |

### Info List

**Info #1**

**86002 SSL Certificate - Information** (1)

# WAS Scan Report

## 86002 SSL Certificate - Information

| | | | |
|---|---|---|---|
| **Finding #** | **4549113**(129546120) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **76240e2d-81ba-420a-88de-18d14d1c775d** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**
SSL certificate information is provided in the Results section.

**Impact**
N/A

**Solution**
N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | 13.53.167.226 |
| **IP** | 13.53.167.226 |
| **Port** | 443 |
| **Result** | #table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _05:d0:96:f9:ca:eb:86:83:69:00:b8:c3:d1:1b:e8:c0:48:aa_ (0)Signature_Algorithm ecdsa-with-SHA384 (0)ISSUER_NAME _ countryName US _organizationName Let's_Encrypt _commonName E5 (0)SUBJECT_NAM commonName api.dictatemed.com (0)Valid_From Jun_24_13:03:53_2025_GMT (0)Valid_Till Sep_22_13:03:52_2025_GMT (0)Public_Key_Algorithm id-ecPublicKey (0)EC_Public_Key (0) _Public-Key:_(256_bit) (0) _pub: (0) _04:7e:f9:49:a2:8e:8c:77:ab:ff:cb:47:3c:65:b8: (0) _93:64:36:17:81:13:c5:62:85:dc:c7:38:6d:2b:ce: (0) _21:6b:7e:d0:21:e8:d6:bf:ad:b2:a4:de:e7:26:aa: (0) _eb:63:28:4c:c2:6e:43:bf:05:41:9a:51:01:bd:39: (0) _3 92:83:df:75 (0) _ASN1_OID:_prime256v1 (0) _NIST_CURVE:_P-256 (0)X509v3_EXTENSIONS _ (0)X509v3_Key_Usage critical (0) _Digital_Signature (0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_Basic_Constraints critical (0) _CA:FALSE (0)X509v3_Subject_Key_Identifier _C7:1A:C0:4B:AC:19:9D:2C:C4:A4:EF:F4:1B:C2:D4:4D:AC:60:72:E8 (0)X509v3_Authority_Key_Identifier _keyid:9F:2B:5F 3C:21:4F:9D:04:B7:ED:2B:2C:C4:C6:70:8B:D2:D7:0D (0)Authority_Information_Access _CA_Issuers_-_URI:http://e5.i.lencr.org/ (0)X509v3_Subject_Alternative_Name _DNS:api.dictatemed.com (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (0)X509v3_CRL_Distribution_Points _Full_Name: (0) _URI:http://e5.c.lencr.org/43.crl (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_A4:42:C5:06:49:60:61:54:8F:0F:D4:EA:9C:FB:7A:2D: (0) _26:45:4D:87:A9:7F:2F:DF:45:59:F6:27:4F:3A:84:54 (0) _Timestamp_:_Jun_24_14:02:23.650_2025_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:46:02:21:00:EB:8A:0A:CC:7D: 51:D7:A0:77:64:8D: (0) _1D:F8:F6:D7:47:6B:C4:02:F8:FD:FC:D0:A4:6A:6E:C1: (0) _A6:02:18:F2:90:02:21:00:AF:BB:78:FC:F8:4A:E1:04: (0) _08:C7:5D: 45:59:12:CB:2A:63:4F:FE:7D:19:78:87:97: (0) _B8:09:0A:7B:51:BE:9F:58 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_CC:FE 6A:85:71:09:65:FE:95:9B:53:CE:E9:B2:7C: (0) _22:E9:85:5C:0D:97:8D:B6:A9:7E:54:C0:FE:4C:0D:B0 (0) _Timestamp_:_Jun_24_14:02:23.665_2025_GMT ( _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:46:02:21:00:B3:0A:86:F9:7A:5D:92:77:6B:06:4D: (0) _0F:A9:E1:D6:03:97:98:B8:53:C9:52:78:76:F8:7B:F9: (0) _08:E7:4E:12:CF:02:21:00:9F:4C:30:B4:20:47:E0:49: (0) _59:F4:BC:F4:E7:93:8D:94:5D: 63:0B:BA:ED:A0:5D:B9: (0) _FC:02:F3:58:70:82:BD:22 (0)Signature (103_octets) (0) 30:65:02:31:00:8a:7c:d7:7d:ef:33:e7:ef:1c:f0:bc (0) 07:57:0a:26:bc:2d:8 43:6e:f2:fd:be:c0:69:ca:9a (0) 78:f4:41:15:c6:0e:60:d4:05:81:c9:00:6a:8c:cc:7d (0) 38:49:b8:fd:33:02:30:64:d6:fe:78:cf:5a:a9:a9:a1 (0) fc:76:34:8c:3c: 76:e8:f8:34:10:88:d2:4e:1a:1d:5c (0) 0b:56:c2:74:33:1c:19:9e:55:b1:03:1f:5e:db:91:8b (0) b3:7c:f1:55:d9:ec:ce:00 (1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _83:8f:6c:63:ce:b1:39:8c:62:06:62:83:15:c9:fd:de_ (1)Signature_Algorithm sha256WithRSAEncryption (1)ISSUER_NAME _ countryName U _organizationName Internet_Security_Research_Group _commonName ISRG_Root_X1 (1)SUBJECT_NAME _ countryName US _organizationName Let's_Encrypt _commonName E5 (1)Valid_From Mar_13_00:00:00_2024_GMT (1)Valid_Till Mar_12_23:59:59_2027_GMT (1)Public_Key_Algorithm id-ecPublicKey (1)EC_Public_Key (1) _Public-Key:_(384_bit) (1) _pub: (1) _04:0d:0b:3a:8a:6b:61:8e:b6:ef:dc:5f:58:e7:c6: (1) _42:45:54:ab:63:f6:66:61:48:0a:2e 59:75:b4:81: (1) _02:37:50:b7:3f:16:79:dc:98:ec:a1:28:97:72:20: (1) _1c:2c:cf:d5:7c:52:20:4e:54:78:5b:84:14:6b:c0: (1) _90:ae:85:ec:c0:51:41:3c:5a:87:7f: 06:4d:d4:fe: (1) _60:d1:fa:6c:2d:e1:7d:95:10:88:a2:08:54:0f:99: (1) _1a:4c:e6:ea:0a:ac:d8 (1) _ASN1_OID:_secp384r1 (1) _NIST_CURVE:_P-384 (1)X509v3_EXTENSIONS _ (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign (1)X509v3_Extended_Key_Usage _TLS_Web_Client_Authentication,_TLS_Web_Server_Authentication (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0 (1)X509v3_Subject_Key_Identifier _9F:2B:5F:CF:3C:21:4F:9D:04:B7:ED:2B:2C:C4:C6:70:8B:D2:D7:0D (1)X509v3_Authority_Key_Identifier _keyid: 79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E (1)Authority_Information_Access _CA_Issuers_-_URI:http://x1.i.lencr.org/ (1)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://x1.c.lencr.org/ (1)Signature (512_octets) (1) 1f:72:9d:34:45:42:41:da:a4:d0:b2:b2:b8:d2:26:4c (1) a7:51:25:8d:42:da:ec:36:48:96:a3:ba:1a:a4:c8:63 (1) d8:f0:2f:b3:ce:cb:9f:67:e9:a0:9e: 19:ea:d4:0d:8a (1) 55:03:92:ca:43:84:9d:46:f1:d5:cc:ba:df:ba:c1:02 (1) 28:71:f7:ba:fe:6d:cc:1b:64:ce:ac:4c:32:1a:12:b8 (1) 91:fc:f2:e4:e8:b2:ac:f4:17:b4:ba: 85:71:80:e2:83 (1) 72:91:bd:b2:f0:f7:dc:9f:86:f4:b7:1f:bf:52:bd:96 (1) e0:e6:49:38:06:e9:73:45:20:de:6f:7c:8e:60:b3:f9 (1) 4c:3f:2a:23:10:c7:48:cc:af:5b:95:c9: 5b:ca (1) c4:ef:16:18:27:23:be:c4:35:9c:9f:cf:c2:df:0b:41 (1) 90:5f:38:5c:95:5c:ff:2e:6c:0a:7f:6a:ed:dd:73:81 (1) 0a:58:6f:4c:3b:9c:dc:c7:5a:93:f7:e3:57:44:67: 5b:11:af:98:11:51:01:a8:dc:88:c7:d7:30:4d:59:b8 (1) 69:a4:df:f1:8e:92:80:0c:ed:99:23:66:69:5e:ca:89 (1) 0f:d4:b1:b3:99:f2:5c:51:df:6c:ed:e7:ae:d7:ff:7f (1) 7a 57:95:77:7f:e7:91:ad:62:30:0c:f8:2e:03:1b (1) 98:bb:79:a3:6a:72:6d:85:fb:2c:58:20:fb:7a:71:b6 (1) ed:61:53:49:08:67:c7:5a:a1:c4:43:81:58:4a:d5:32 (1) |

16:7b:fc:b2:3c:aa:53:cc:a9:81:96:8d:27:d6:95:71 (1) 64:88:08:b3:88:13:5f:d0:bf:fe:e8:2a:c9:d9:09:62 (1) 7d:db:ac:14:e9:1a:86:d4:e6:0f:18:e8:b5:ce:e0:01 (1) 3a:d5:cb:8f:54:34:f6:f2:74:12:fd:ee:b3:f7 (1) 97:09:5e:ad:1e:2b:50:5c:68:9e:9f:25:9b:26:6e:34 (1) 60:0f:9a:77:9a:f1:1f:e6:f7:50:33:b3:02:12:f5:34 (1) b4:76:ec:c7:62:39:98:71:c9:a0:00:47:6f:c2:95:06 (1) 05:a9:fe:57:17:19:68:96:69:e3:b2:07:b4:4f:f8:e7 (1) c3:b6:f8:b6:3a:c6:a9:c5:78:95:ee:f3:55:b3:b7:cc (1) 96:b4:63:63:58:e8:29:aa:a6:9b:27:27:06:f0:2a:d7 (1) 80:04:6e:dc:8b:b1:57:ce:4b:ae:81:f1:aa:64:78:55 (1) f6:35:8e:17:3c:46:15:e1:94:82:7b:c5:47:3e:b7:6b (1) 11:19:36:c0:82:c6:dd:3f:c4:1a:64:88:90:26:15:50 (1) c4:a7:8e:62:5d:55:00:fd:17:a3:5a:ff:ec:e6:5c:27

## Info List

### Info #1

Certificate Fingerprint:5DFDB3CF31B26F23D87C09F3A0CEF642F64069A9FB7CFE29270BB5DC0F1E16BB

### 150006 Web Application Authentication Not Attempted (1)

150006 Web Application Authentication Not Attempted

| | | | |
|---|---|---|---|
| **Finding #** | **4549107**(129546114) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **142390d4-79bc-47c3-b134-640bcb0cfc28** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

#### Details

**Threat**

Web application authentication was enabled for the scan, but it was not performed for this particular host. It was not performed because a login page was not discovered, or a login page was discovered that submits via HTTP and the scan configuration requires that credentials be submitted via HTTPS.

**Impact**

Vulnerabilities that require authentication may not be detected.

**Solution**

To allow web application authentication to this host, use an appropriate authentication record and ensure the login page is in the crawl scope. Also, if the web application does not support HTTPS, the scan configuration needs to allow transmission of credentials over plaintext HTTP connections.

#### Results

Application authentication was specified, but no login forms were discovered during the crawl.

### 150009 Links Crawled (1)

# WAS Scan Report

## 150009 Links Crawled

| | | | |
|---|---|---|---|
| **Finding #** | **4549110**(129546117) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **08b2b0f8-e3bb-4cc2-8c73-f4b5994b6017** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

### Impact

N/A

### Solution

N/A

## Results

Duration of crawl phase (seconds): 305.00
Number of links: 40
(This number excludes form requests and links re-requested during authentication.)

https://api.dictatemed.com/api/v1
https://api.dictatemed.com/api/v1/
https://api.dictatemed.com/api/v1/2fa/totp/generate
https://api.dictatemed.com/api/v1/2fa/totp/verify
https://api.dictatemed.com/api/v1/audit/log
https://api.dictatemed.com/api/v1/audit/logs
https://api.dictatemed.com/api/v1/auth/change-password
https://api.dictatemed.com/api/v1/auth/forgot-password
https://api.dictatemed.com/api/v1/auth/refresh-token
https://api.dictatemed.com/api/v1/auth/reset-password
https://api.dictatemed.com/api/v1/auth/signin
https://api.dictatemed.com/api/v1/auth/signup
https://api.dictatemed.com/api/v1/auth/verify/email
https://api.dictatemed.com/api/v1/chunking/start-recording
https://api.dictatemed.com/api/v1/chunking/upload-chunk
https://api.dictatemed.com/api/v1/chunking/upload-merged
https://api.dictatemed.com/api/v1/classifications
https://api.dictatemed.com/api/v1/classifications/123e4567-e89b-12d3-a456-426614174003
https://api.dictatemed.com/api/v1/dictations
https://api.dictatemed.com/api/v1/dictations/123e4567-e89b-12d3-a456-426614174002
https://api.dictatemed.com/api/v1/dictations/full-dictaion
https://api.dictatemed.com/api/v1/dictations/statics
https://api.dictatemed.com/api/v1/dictations/update/dictation
https://api.dictatemed.com/api/v1/dictations/upload
https://api.dictatemed.com/api/v1/email/send
https://api.dictatemed.com/api/v1/email/send-with-attachment
https://api.dictatemed.com/api/v1/my/classifications
https://api.dictatemed.com/api/v1/my/classifications/123e4567-e89b-12d3-a456-426614174001
https://api.dictatemed.com/api/v1/s3bucket/generatePresignedUrl
https://api.dictatemed.com/api/v1/s3bucket/sample-file-key-123
https://api.dictatemed.com/api/v1/s3bucket/upload
https://api.dictatemed.com/api/v1/settings
https://api.dictatemed.com/api/v1/settings/123e4567-e89b-12d3-a456-426614174000
https://api.dictatemed.com/api/v1/settings/me
https://api.dictatemed.com/api/v1/user/create-user
https://api.dictatemed.com/api/v1/user/me
https://api.dictatemed.com/api/v1/user/update-user
https://api.dictatemed.com/favicon.ico

# WAS Scan Report

http://api.dictatemed.com/api/v1/
http://api.dictatemed.com/favicon.ico

## 150020 Links Rejected By Crawl Scope or Exclusion List (1)

### 150020 Links Rejected By Crawl Scope or Exclusion List

| | | | |
|---|---|---|---|
| **Finding #** | **4549101**(129546108) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **d09e60f1-4fad-41af-abb0-5cb4634e94a1** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

**Impact**

Links listed here were neither crawled or tested by the Web application scanning engine.

**Solution**

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

### Results

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

IP based excluded links:

## 150021 Scan Diagnostics (1)

# WAS Scan Report

## 150021 Scan Diagnostics

| | | | |
|---|---|---|---|
| **Finding #** | **4549103**(129546110) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **b0491421-5f84-4eca-893d-4951defffda1** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

### Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

### Solution

No action is required.

## Results

Loaded 0 exclude list entries.
Loaded 0 allow list entries.
Target web application page https://api.dictatemed.com/api/v1 fetched. Status code:302, Content-Type:text/html, load time:1 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 VirtualHostDiscovery: estimated time < 10 minutes (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 69 requests, 31 seconds. Completed 69 requests of 70 estimated requests (98.5714%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 56 requests, 8 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
Batch #0 ApiSec spec files detection: estimated time < 1 minute (1 tests, 1 inputs)
ApiSec spec files detection: 1 vulnsigs tests, completed 0 requests, 16 seconds. No tests to execute.
Collected 40 links overall in 0 hours 5 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
WS Directory Path manipulation no tests enabled.
Batch #0 WS enumeration: estimated time < 10 minutes (11 tests, 59 inputs)
WS enumeration: 11 vulnsigs tests, completed 264 requests, 10 seconds. Completed 264 requests of 649 estimated requests (40.678%). All tests completed.
Batch #4 WebCgiOob: estimated time < 10 minutes (167 tests, 1 inputs)
Batch #4 WebCgiOob: 167 vulnsigs tests, completed 149 requests, 8 seconds. Completed 149 requests of 1711 estimated requests (8.70836%). All tests completed.
Potential LDAP Login Bypass no tests enabled.
Insufficient Authentication token validation no tests enabled.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 40 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 40 estimated requests (0%). All tests completed.
Header manipulation no tests enabled.
shell shock detector no tests enabled.
httpoxy no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 200 requests, 37 seconds. No tests to execute.
Path XSS manipulation no tests enabled.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation no tests enabled.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 30 minutes (1461 tests, 1 inputs)
Batch #5 WebCgiGeneric: 1461 vulnsigs tests, completed 1964 requests, 101 seconds. Completed 1964 requests of 22479 estimated requests (8.73704%). All tests completed.
WebCgiTimebasedTests: no test enabled
Open Redirect no tests enabled.

# WAS Scan Report

Duration of Crawl Time: 305.00 (seconds)
Duration of Test Phase: 831.00 (seconds)
Total Scan Time: 1136.00 (seconds)

Total requests made: 3020
Average server response time: 0.18 seconds

Average browser load time: 0.17 seconds

## 150308 Explicit URLs Specified (1)

# WAS Scan Report

## 150308 Explicit URLs Specified

| | | | |
|---|---|---|---|
| **Finding #** | **4549102**(129546109) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **0d2398ca-dc21-4b27-94f2-8806710dd595** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

Explicit URLs specified in the web application profile are listed in the Results section. These URLs were provided as part of the overall scan configuration and added to the crawl queue to be crawled first.

**Impact**

N/A

**Solution**

N/A

### Results

Explicit links specified.
Number of links: 35
https://api.dictatemed.com/api/v1/settings
https://api.dictatemed.com/api/v1/settings/123e4567-e89b-12d3-a456-426614174000
https://api.dictatemed.com/api/v1/my/classifications
https://api.dictatemed.com/api/v1/my/classifications/123e4567-e89b-12d3-a456-426614174001
https://api.dictatemed.com/api/v1/dictations
https://api.dictatemed.com/api/v1/dictations/123e4567-e89b-12d3-a456-426614174002
https://api.dictatemed.com/api/v1/classifications
https://api.dictatemed.com/api/v1/classifications/123e4567-e89b-12d3-a456-426614174003
https://api.dictatemed.com/api/v1/user/me
https://api.dictatemed.com/api/v1/user/update-user
https://api.dictatemed.com/api/v1/user/create-user
https://api.dictatemed.com/api/v1/s3bucket/upload
https://api.dictatemed.com/api/v1/s3bucket/generatePresignedUrl
https://api.dictatemed.com/api/v1/s3bucket/sample-file-key-123
https://api.dictatemed.com/api/v1/email/send
https://api.dictatemed.com/api/v1/email/send-with-attachment
https://api.dictatemed.com/api/v1/dictations/upload
https://api.dictatemed.com/api/v1/dictations/update/dictation
https://api.dictatemed.com/api/v1/dictations/full-dictaion
https://api.dictatemed.com/api/v1/dictations/statics
https://api.dictatemed.com/api/v1/chunking/upload-merged
https://api.dictatemed.com/api/v1/chunking/upload-chunk
https://api.dictatemed.com/api/v1/chunking/start-recording
https://api.dictatemed.com/api/v1/auth/verify/email
https://api.dictatemed.com/api/v1/auth/signup
https://api.dictatemed.com/api/v1/auth/signin
https://api.dictatemed.com/api/v1/auth/reset-password
https://api.dictatemed.com/api/v1/auth/refresh-token
https://api.dictatemed.com/api/v1/auth/forgot-password
https://api.dictatemed.com/api/v1/auth/change-password
https://api.dictatemed.com/api/v1/audit/log
https://api.dictatemed.com/api/v1/audit/logs
https://api.dictatemed.com/api/v1/2fa/totp/verify
https://api.dictatemed.com/api/v1/2fa/totp/generate
https://api.dictatemed.com/api/v1/settings/me

## 150454 Scan Configuration Suggestions (1)

# WAS Scan Report

## 150454 Scan Configuration Suggestions

| | | | |
|---|---|---|---|
| **Finding #** | **4549108**(129546115) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **ccb74515-554b-463a-9b8e-09e265c284a4** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

#### Threat

Results section lists configuration improvements for the scan that will help WAS to optimize the crawling and testing of the application.
WAS scan will determine Swagger 2.0, OpenAPI 3.0.x specifications URLs during crawling. All the those links will be reported in results section of this QID.
WAS scan will crawl and analyze the presence of authentication form, due to various factors scan may not be able to identify login page. Few reasons for not identifying login page could be form is not using traditional username/password fields, login page is hidden, login form was not crawled (review QID 150009, 150115), access to the login page was not correctly configured (review response code in 150546 if login page was configured as starting URL) or scanner may have redirected to SSO page. In such cases, it is recommended to use selenium authentication and review results to ensure login page is authenticated successfully.

#### Impact

Because of unoptimized configuration certain parts of the web application are not covered or more time is spent on the redundant parts of the application.
Swagger 2.0, OpenAPI 3.0.x will have typical end points, those APIs to be tested for vulnerabilities should be configured as a separate scan.
Most vulnerabilities reside post authentication, it is important to configure web application aptly to detect vulnerabilities on links that are otherwise available after authentication only.

#### Solution

Consider the suggested improvements for better coverage and optimize the scan with better results. For more details refer to https://success.qualys.com/support/s/article/000006263

### Results

Application authentication was specified, but no login forms were discovered during the crawl. Please use selenium authentication once.

## 150528 Server Returns HTTP 4XX Error Code During Scanning (1)

# WAS Scan Report

## 150528 Server Returns HTTP 4XX Error Code During Scanning

| | | | |
|---|---|---|---|
| **Finding #** | **4549100**(129546107) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **efb3ae50-dce6-4780-806c-3cbf11023949** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat

During the WAS scan, one of the request to links listed in results section of this QID resulted with HTTP 4xx response code. The list of supported 4xx response code are as below:

400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not Found
405 - Method Not Allowed
407 - Proxy Authentication Required
408 - Request Timeout
413 - Payload Too Large
414 - URI Too Long
Refer to QIDs 150009, 150148, 150152, and 150172 to check for the links scanned in the application. Links reported in 150528, if present in the above QIDs, indicate that the links were scanned.

### Impact

The presence of a HTTP 4xx response during the crawl phase indicates that one of the requests to the link did not result in retrieving the content of that link. WAS depends on responses to detect many vulnerabilities on that link. If the link does not respond with an expected response during the scan vulnerabilities present on such links may not be detected.

### Solution

Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

## Results

Number of links with 4xx response code: 29
(Only first 50 such links are listed)

401 https://api.dictatemed.com/api/v1/
401 https://api.dictatemed.com/api/v1/2fa/totp/generate
401 https://api.dictatemed.com/api/v1/2fa/totp/verify
401 https://api.dictatemed.com/api/v1/audit/log
401 https://api.dictatemed.com/api/v1/audit/logs
401 https://api.dictatemed.com/api/v1/chunking/start-recording
401 https://api.dictatemed.com/api/v1/chunking/upload-chunk
401 https://api.dictatemed.com/api/v1/chunking/upload-merged
401 https://api.dictatemed.com/api/v1/classifications
401 https://api.dictatemed.com/api/v1/classifications/123e4567-e89b-12d3-a456-426614174003
401 https://api.dictatemed.com/api/v1/dictations
401 https://api.dictatemed.com/api/v1/dictations/123e4567-e89b-12d3-a456-426614174002
401 https://api.dictatemed.com/api/v1/dictations/full-dictaion
401 https://api.dictatemed.com/api/v1/dictations/statics
401 https://api.dictatemed.com/api/v1/dictations/upload
401 https://api.dictatemed.com/api/v1/email/send
401 https://api.dictatemed.com/api/v1/email/send-with-attachment
401 https://api.dictatemed.com/api/v1/my/classifications
401 https://api.dictatemed.com/api/v1/my/classifications/123e4567-e89b-12d3-a456-426614174001
401 https://api.dictatemed.com/api/v1/s3bucket/generatePresignedUrl
401 https://api.dictatemed.com/api/v1/s3bucket/sample-file-key-123
401 https://api.dictatemed.com/api/v1/s3bucket/upload
401 https://api.dictatemed.com/api/v1/settings
401 https://api.dictatemed.com/api/v1/settings/123e4567-e89b-12d3-a456-426614174000
401 https://api.dictatemed.com/api/v1/settings/me
401 https://api.dictatemed.com/api/v1/user/create-user
401 https://api.dictatemed.com/api/v1/user/me
401 https://api.dictatemed.com/api/v1/user/update-user

404 https://api.dictatemed.com/favicon.ico

## 150546 First Link Crawled Response Code Information (1)

### 150546 First Link Crawled Response Code Information

| | | | |
|---|---|---|---|
| **Finding #** | **4549106**(129546113) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **b1f85e25-4e22-42b9-ac56-11410f885ef8** | | |
| **Group** | Scan Diagnostics | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

#### Details

**Threat**

The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

**Impact**

An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

**Solution**

Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

#### Results

Base URI: https://api.dictatemed.com/api/v1
Response Code: 302
Response Header:
date: Mon, 28 Jul 2025 08:27:04 GMT
location: http://api.dictatemed.com/api/v1/
server: nginx/1.26.3
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
x-frame-options: DENY

Response Body:
<html><head></head><body></body></html>

## Security Weaknesses (5)

### 150210 Information Disclosure via Response Header (1)

# WAS Scan Report

## 150210 Information Disclosure via Response Header

| | | | |
|---|---|---|---|
| **Finding #** | **4549098**(129546105) | **Severity** | Information Gathered - Level 3 |
| **Unique #** | **e1426edb-17dc-4fbc-b385-8fbd46f799af** | | |
| **Group** | Security Weaknesses | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | CWE-16, CWE-201 | | |
| **OWASP** | A5 Security Misconfiguration | | |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | | |

### Details

#### Threat

HTTP response headers like 'Server', 'X-Powered-By', 'X-AspNetVersion', 'X-AspNetMvcVersion' could disclose information about the platform and technologies used by the website. The HTTP response include one or more such headers.

#### Impact

The headers can potentially be used by attackers for fingerprinting and launching attacks specific to the technologies and versions used by the web application. These response headers are not necessary for production sites and should be disabled.

#### Solution

Disable such response headers, remove them from the response, or make sure that the header value does not contain information which could be used to fingerprint the server-side components of the web application.

### Results

One or more response headers disclosing information about the application platform were present on the following pages:
(Only first 50 such pages are reported)

GET https://api.dictatemed.com/api/v1/settings response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/settings/123e4567-e89b-12d3-a456-426614174000 response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/my/classifications response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/my/classifications/123e4567-e89b-12d3-a456-426614174001 response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/dictations response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/dictations/123e4567-e89b-12d3-a456-426614174002 response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/classifications response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/classifications/123e4567-e89b-12d3-a456-426614174003 response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/user/me response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/user/update-user response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/user/create-user response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/s3bucket/upload response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/s3bucket/generatePresignedUrl response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/s3bucket/sample-file-key-123 response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/email/send response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/email/send-with-attachment response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/dictations/upload response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/dictations/update/dictation response code: 500
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/dictations/full-dictaion response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/dictations/statics response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/chunking/upload-merged response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/chunking/upload-chunk response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/chunking/start-recording response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/auth/verify/email response code: 500
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/auth/signup response code: 500
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/auth/signin response code: 500
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/auth/reset-password response code: 500
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/auth/refresh-token response code: 500
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/auth/forgot-password response code: 500
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/auth/change-password response code: 500
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/audit/log response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/audit/logs response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/2fa/totp/verify response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/2fa/totp/generate response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/settings/me response code: 401
server: nginx/1.26.3

GET https://api.dictatemed.com/favicon.ico response code: 404
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1 response code: 302
server: nginx/1.26.3

GET https://api.dictatemed.com/api/v1/ response code: 401
server: nginx/1.26.3



## 150206 Content-Security-Policy Not Implemented (1)

# WAS Scan Report

## 150206 Content-Security-Policy Not Implemented

| | | | |
|---|---|---|---|
| **Finding #** | **4549111**(129546118) | **Severity** | Information Gathered - Level 2 |
| **Unique #** | **86855bf9-c573-4159-ac85-546fcc436041** | | |
| **Group** | Security Weaknesses | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | CWE-16, CWE-1032 | | |
| **OWASP** | A5 Security Misconfiguration | | |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | | |

## Details

### Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

### Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

### Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

## Results

Content-Security-Policy: Header missing
Response headers on link: GET https://api.dictatemed.com/api/v1/settings response code: 401
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 95
content-type: application/json;charset=UTF-8
date: Mon, 28 Jul 2025 08:24:43 GMT
expires: 0
pragma: no-cache
server: nginx/1.26.3
strict-transport-security: max-age=31536000; includeSubDomains
vary: Origin
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 0

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://api.dictatemed.com/api/v1/settings response code: 401
GET https://api.dictatemed.com/api/v1/settings/123e4567-e89b-12d3-a456-426614174000 response code: 401
GET https://api.dictatemed.com/api/v1/my/classifications response code: 401
GET https://api.dictatemed.com/api/v1/my/classifications/123e4567-e89b-12d3-a456-426614174001 response code: 401
GET https://api.dictatemed.com/api/v1/dictations response code: 401
GET https://api.dictatemed.com/api/v1/dictations/123e4567-e89b-12d3-a456-426614174002 response code: 401
GET https://api.dictatemed.com/api/v1/classifications response code: 401

GET https://api.dictatemed.com/api/v1/classifications/123e4567-e89b-12d3-a456-426614174003 response code: 401
GET https://api.dictatemed.com/api/v1/user/me response code: 401
GET https://api.dictatemed.com/api/v1/user/update-user response code: 401
GET https://api.dictatemed.com/api/v1/user/create-user response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/upload response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/generatePresignedUrl response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/sample-file-key-123 response code: 401
GET https://api.dictatemed.com/api/v1/email/send response code: 401
GET https://api.dictatemed.com/api/v1/email/send-with-attachment response code: 401
GET https://api.dictatemed.com/api/v1/dictations/upload response code: 401
GET https://api.dictatemed.com/api/v1/dictations/update/dictation response code: 500
GET https://api.dictatemed.com/api/v1/dictations/full-dictaion response code: 401
GET https://api.dictatemed.com/api/v1/dictations/statics response code: 401
GET https://api.dictatemed.com/api/v1/chunking/upload-merged response code: 401
GET https://api.dictatemed.com/api/v1/chunking/upload-chunk response code: 401
GET https://api.dictatemed.com/api/v1/chunking/start-recording response code: 401
GET https://api.dictatemed.com/api/v1/auth/verify/email response code: 500
GET https://api.dictatemed.com/api/v1/auth/signup response code: 500
GET https://api.dictatemed.com/api/v1/auth/signin response code: 500
GET https://api.dictatemed.com/api/v1/auth/reset-password response code: 500
GET https://api.dictatemed.com/api/v1/auth/refresh-token response code: 500
GET https://api.dictatemed.com/api/v1/auth/forgot-password response code: 500
GET https://api.dictatemed.com/api/v1/auth/change-password response code: 500
GET https://api.dictatemed.com/api/v1/audit/log response code: 401
GET https://api.dictatemed.com/api/v1/audit/logs response code: 401
GET https://api.dictatemed.com/api/v1/2fa/totp/verify response code: 401
GET https://api.dictatemed.com/api/v1/2fa/totp/generate response code: 401
GET https://api.dictatemed.com/api/v1/settings/me response code: 401
GET https://api.dictatemed.com/favicon.ico response code: 404
GET https://api.dictatemed.com/api/v1/ response code: 401



## 150208 Missing header: Referrer-Policy (1)

# WAS Scan Report

## 150208 Missing header: Referrer-Policy

| | | | |
|---|---|---|---|
| **Finding #** | **4549099**(129546106) | **Severity** | Information Gathered - Level 2 |
| **Unique #** | **94a7366d-172d-4b18-84e2-12fbb0aad247** | | |
| **Group** | Security Weaknesses | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | CWE-16, CWE-1032 | | |
| **OWASP** | A5 Security Misconfiguration | | |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | | |

## Details

### Threat

The Referrer Policy header is used to control the flow of information from the source to the destination when a link is clicked. During the scan checks are done for the presence of the Referrer Policy on all static and dynamic pages. One of the following values for Referrer Policy in the response headers was found to be missing:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found, the response body is checked for a meta tag containing the tag name as "referrer" and one of the above Referrer Policy. Missing referrer header is reported for links with the following response codes - 2XX, 4xx, and 5xx. Links that report a response code of 3xx will not be tested for presence of this header.

### Impact

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

### Solution

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

## Results

Referrer-Policy: Header missing
Response headers on link: GET https://api.dictatemed.com/api/v1/settings response code: 401
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 95
content-type: application/json;charset=UTF-8
date: Mon, 28 Jul 2025 08:24:43 GMT
expires: 0
pragma: no-cache
server: nginx/1.26.3
strict-transport-security: max-age=31536000; includeSubDomains
vary: Origin
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 0

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://api.dictatemed.com/api/v1/settings response code: 401
GET https://api.dictatemed.com/api/v1/settings/123e4567-e89b-12d3-a456-426614174000 response code: 401
GET https://api.dictatemed.com/api/v1/my/classifications response code: 401
GET https://api.dictatemed.com/api/v1/my/classifications/123e4567-e89b-12d3-a456-426614174001 response code: 401

GET https://api.dictatemed.com/api/v1/dictations response code: 401
GET https://api.dictatemed.com/api/v1/dictations/123e4567-e89b-12d3-a456-426614174002 response code: 401
GET https://api.dictatemed.com/api/v1/classifications response code: 401
GET https://api.dictatemed.com/api/v1/classifications/123e4567-e89b-12d3-a456-426614174003 response code: 401
GET https://api.dictatemed.com/api/v1/user/me response code: 401
GET https://api.dictatemed.com/api/v1/user/update-user response code: 401
GET https://api.dictatemed.com/api/v1/user/create-user response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/upload response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/generatePresignedUrl response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/sample-file-key-123 response code: 401
GET https://api.dictatemed.com/api/v1/email/send response code: 401
GET https://api.dictatemed.com/api/v1/email/send-with-attachment response code: 401
GET https://api.dictatemed.com/api/v1/dictations/upload response code: 401
GET https://api.dictatemed.com/api/v1/dictations/update/dictation response code: 500
GET https://api.dictatemed.com/api/v1/dictations/full-dictaion response code: 401
GET https://api.dictatemed.com/api/v1/dictations/statics response code: 401
GET https://api.dictatemed.com/api/v1/chunking/upload-merged response code: 401
GET https://api.dictatemed.com/api/v1/chunking/upload-chunk response code: 401
GET https://api.dictatemed.com/api/v1/chunking/start-recording response code: 401
GET https://api.dictatemed.com/api/v1/auth/verify/email response code: 500
GET https://api.dictatemed.com/api/v1/auth/signup response code: 500
GET https://api.dictatemed.com/api/v1/auth/signin response code: 500
GET https://api.dictatemed.com/api/v1/auth/reset-password response code: 500
GET https://api.dictatemed.com/api/v1/auth/refresh-token response code: 500
GET https://api.dictatemed.com/api/v1/auth/forgot-password response code: 500
GET https://api.dictatemed.com/api/v1/auth/change-password response code: 500
GET https://api.dictatemed.com/api/v1/audit/log response code: 401
GET https://api.dictatemed.com/api/v1/audit/logs response code: 401
GET https://api.dictatemed.com/api/v1/2fa/totp/verify response code: 401
GET https://api.dictatemed.com/api/v1/2fa/totp/generate response code: 401
GET https://api.dictatemed.com/api/v1/settings/me response code: 401
GET https://api.dictatemed.com/favicon.ico response code: 404
GET https://api.dictatemed.com/api/v1/ response code: 401



## 150248 Missing header: Permissions-Policy (1)

# WAS Scan Report

## 150248 Missing header: Permissions-Policy

| | | | |
|---|---|---|---|
| **Finding #** | **4549104**(129546111) | **Severity** | Information Gathered - Level 2 |
| **Unique #** | **69324f07-2094-40c3-ab46-aba316a0b5d2** | | |
| **Group** | Security Weaknesses | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | CWE-284 | | |
| **OWASP** | A5 Security Misconfiguration | | |
| **WASC** | - | | |

## Details

### Threat
The Permissions-Policy response header is not present.

### Impact
Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

### Solution
It is recommended to define policy for policy controlled features to make application more secure.

References:
Permissions-Policy W3C Working Draft
Policy Controlled Features

## Results

Permissions-Policy: Header missing
Response headers on link: GET https://api.dictatemed.com/api/v1/settings response code: 401
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 95
content-type: application/json;charset=UTF-8
date: Mon, 28 Jul 2025 08:24:43 GMT
expires: 0
pragma: no-cache
server: nginx/1.26.3
strict-transport-security: max-age=31536000; includeSubDomains
vary: Origin
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 0

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://api.dictatemed.com/api/v1/settings response code: 401
GET https://api.dictatemed.com/api/v1/settings/123e4567-e89b-12d3-a456-426614174000 response code: 401
GET https://api.dictatemed.com/api/v1/my/classifications response code: 401
GET https://api.dictatemed.com/api/v1/my/classifications/123e4567-e89b-12d3-a456-426614174001 response code: 401
GET https://api.dictatemed.com/api/v1/dictations response code: 401
GET https://api.dictatemed.com/api/v1/dictations/123e4567-e89b-12d3-a456-426614174002 response code: 401
GET https://api.dictatemed.com/api/v1/classifications response code: 401
GET https://api.dictatemed.com/api/v1/classifications/123e4567-e89b-12d3-a456-426614174003 response code: 401
GET https://api.dictatemed.com/api/v1/user/me response code: 401
GET https://api.dictatemed.com/api/v1/user/update-user response code: 401
GET https://api.dictatemed.com/api/v1/user/create-user response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/upload response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/generatePresignedUrl response code: 401
GET https://api.dictatemed.com/api/v1/s3bucket/sample-file-key-123 response code: 401
GET https://api.dictatemed.com/api/v1/email/send response code: 401
GET https://api.dictatemed.com/api/v1/email/send-with-attachment response code: 401
GET https://api.dictatemed.com/api/v1/dictations/upload response code: 401
GET https://api.dictatemed.com/api/v1/dictations/update/dictation response code: 500
GET https://api.dictatemed.com/api/v1/dictations/full-dictaion response code: 401

GET https://api.dictatemed.com/api/v1/dictations/statics response code: 401
GET https://api.dictatemed.com/api/v1/chunking/upload-merged response code: 401
GET https://api.dictatemed.com/api/v1/chunking/upload-chunk response code: 401
GET https://api.dictatemed.com/api/v1/chunking/start-recording response code: 401
GET https://api.dictatemed.com/api/v1/auth/verify/email response code: 500
GET https://api.dictatemed.com/api/v1/auth/signup response code: 500
GET https://api.dictatemed.com/api/v1/auth/signin response code: 500
GET https://api.dictatemed.com/api/v1/auth/reset-password response code: 500
GET https://api.dictatemed.com/api/v1/auth/refresh-token response code: 500
GET https://api.dictatemed.com/api/v1/auth/forgot-password response code: 500
GET https://api.dictatemed.com/api/v1/auth/change-password response code: 500
GET https://api.dictatemed.com/api/v1/audit/log response code: 401
GET https://api.dictatemed.com/api/v1/audit/logs response code: 401
GET https://api.dictatemed.com/api/v1/2fa/totp/verify response code: 401
GET https://api.dictatemed.com/api/v1/2fa/totp/generate response code: 401
GET https://api.dictatemed.com/api/v1/settings/me response code: 401
GET https://api.dictatemed.com/favicon.ico response code: 404
GET https://api.dictatemed.com/api/v1/ response code: 401

## 150126 Links With High Resource Consumption (1)

### 150126 Links With High Resource Consumption

| | | | |
|---|---|---|---|
| **Finding #** | **4549105**(129546112) | **Severity** | Information Gathered - Level 1 |
| **Unique #** | **be1e426b-b558-4d06-beb4-df5be5e4c49f** | | |
| **Group** | Security Weaknesses | **Detection Date** | 28 Jul 2025 13:54 GMT+0630 |
| **CWE** | - | | |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

#### Threat

The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

#### Impact

The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

#### Solution

Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

### Results

593.700000 bytes/sec https://api.dictatemed.com/api/v1/2fa/totp/verify
635.900000 bytes/sec https://api.dictatemed.com/api/v1/s3bucket/upload
636.700000 bytes/sec https://api.dictatemed.com/api/v1/chunking/upload-merged
636.700000 bytes/sec https://api.dictatemed.com/api/v1/email/send
637.000000 bytes/sec https://api.dictatemed.com/api/v1/dictations/123e4567-e89b-12d3-a456-426614174002
637.700000 bytes/sec https://api.dictatemed.com/api/v1/my/classifications
637.700000 bytes/sec https://api.dictatemed.com/api/v1/user/me
637.800000 bytes/sec https://api.dictatemed.com/api/v1/settings
745.500000 bytes/sec https://api.dictatemed.com/api/v1/auth/reset-password
747.400000 bytes/sec https://api.dictatemed.com/api/v1/dictations/update/dictation

# WAS Scan Report

## Appendix

### Scan Details

#### Jul 28, 2025

| | |
|---|---|
| Reference | was/1753690954802.4227079 |
| Date | 28 Jul 2025 13:54 GMT+0630 |
| Mode | On-Demand |
| Progressive Scanning | Disabled |
| Type | Vulnerability |
| Authentication | Default Login |
| Scanner Appliance | External (IP: 168.138.113.116, Scanner: 0.6.680b2-1, WAS: 10.10.0-1, Signatures: 2.6.376-3) |
| Profile | API Compliance Options |
| DNS Override | - |
| Duration | 00:20:54 |
| Status | Finished |
| Authentication Status | Not used |

### Option Profile Details

| | |
|---|---|
| Form Submission | BOTH |
| Form Crawl Scope | Do not include form action URI in uniqueness calculation |
| Maximum links to test in scope | 300 |
| User Agent | - |
| Request Parameter Set | Initial Parameters |
| Document Type | Do not ignore common binary files |
| Enhanced Crawling | Disabled |
| SmartScan | Disabled |
| Timeout Error Threshold | 100 |
| Unexpected Error Threshold | 300 |
| Performance Settings | Pre-defined |
| Scan Intensity | Low |
| Bruteforce Option | Minimal |
| Detection Scope | Categories |
| Include additional XSS payloads | No |
| Search List Categories | API Compliance, OWASP API TOP 10 |
| Inclusion Search List QIDs | 152429, 580504, 570008, 570009, 580505, 570010, 580506, 570011, 580507, 570012, 580508, 570013, 580509, 570014, 580510, 570015, 580511, 570001, 570002, 570003, 570004, 570005, 580502, 570007, 580503, 570024, 580520, 570025, 580521, 570026, 580522, 570027, 580523, 570028, 580524, 580525, 570029, 570030, 580526, 570031, 580527, 570016, 580512, 580513, 570017, 570018, 580514, 580515, 570019, 570020, 580516, 570021, 580517, 580518, 570022, 570023, 580519, 580536, 570040, 570041, 580537, 580538, 570042, 570043, 580539, 570044, 580540, 570045, 580541, 570046, 580542, 580543, 570047, 570032, 580528, 570033, 580529, 570034, 580530, 580531, 570035, 570036, 580532, 570037, 580533, 570038, 580534, 580535, 570039, 570056, 580552, 570057, 580553, 580554, 570058, 570059, 580555, 580556, 570060, 580557, 570061, 570062, 580558, 580559, 570063, 580544, 570049, 580545, 570050, 580546, 570051, 580547, 580548, 570052, 580549, 570053, 570054, 580550, 580551, 570055, 570072, 570073, 570074, 570075, 570076, 570077, 570078, 570079, 580560, 570064, 570065, 580561, 580562, 570066, 570067, 580563, 570068, 580564, 570069, 570070, 570071, 570088, 570089, 570090, 570091, 570092, 570093, 570094, 570095, 570080, 570081, 570082, 570083, 570084, |

570085, 570086, 570087, 570096, 570097, 570098, 570099, 151053, 152592, 150557, 152611, 150563, 150055, 152622, 150574, 150581, 152121, 150596, 530014, 530001, 530004, 530025, 530027, 530022, 152690, 152694, 152703, 152189, 530056, 152707, 530061, 530053, 530054, 150668, 152716, 152722, 530064, 152730, 152218, 570001, 570002, 570003, 570007, 152738, 152739, 530090, 152736, 152737, 152743, 150692, 530095, 150693, 152744, 152750, 530086, 150701, 530109, 570045, 152756, 570046, 530097, 530102, 570058, 570059, 570060, 570061, 570062, 530127, 570063, 580800, 152779, 570051, 152782, 570052, 152780, 570054, 152269, 152781, 152786, 570072, 570073, 570074, 570075, 570077, 150740, 530142, 152788, 570078, 570079, 530128, 570064, 530130, 570066, 570067, 152798, 570068, 570069, 570070, 152797, 570071, 152803, 152801, 152294, 152293, 570080, 152811, 570081, 570082, 570083, 530148, 570084, 530151, 152818, 152817, 152822, 152821, 152309, 570098, 570099, 152318, 152835, 530186, 152839, 152836, 152842, 152843, 150795, 152841, 152846, 530181, 152847, 530182, 152851, 152854, 152855, 152853, 530192, 152858, 530193, 152859, 152857, 152863, 530198, 530199, 152861, 152866, 152865, 152870, 150823, 152871, 152868, 152869, 150824, 152879, 150828, 152877, 152365, 530234, 152886, 152372, 152885, 152890, 152891, 152888, 530227, 152889, 152892, 152899, 152896, 152902, 530255, 152901, 152392, 152910, 152912, 152919, 152927, 152412, 520045, 152942, 152940, 152941, 520055, 152959, 150915, 152961, 530318, 152453, 152459, 152969, 530308, 152972, 152460, 150931, 152977, 150933, 530321, 152991, 150943, 152476, 152989, 152477, 152480, 152487, 152996, 152997, 153002, 153006, 580539, 580541, 580542, 152506, 152514, 580553, 580554, 580556, 580557, 580559, 580544, 580545, 580547, 580548, 580550, 580551, 150992, 580560, 580562, 580563, 580565, 580566, 152540, 152028, 152547, 152033, 152548, 152566, 152564, 150011, 151039, 150524, 151036

| | |
|---|---|
| Credit Card Numbers Search | Off |
| Social Security Numbers (US) Search | Off |

## Web Application Details: DictateMed API 2

| | |
|---|---|
| Name | DictateMed API 2 |
| ID | 68839344 |
| URL | https://api.dictatemed.com/api/v1 |
| Owner | Tibu Padmakumar (craka8tp) |
| Scope | Limit to URL hostname |
| Tags | - |
| Custom Attributes | - |

## Severity Levels

### Confirmed Vulnerabilities

Vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

| | |
|---|---|
| Minimal | Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find. |
| Medium | Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories. |
| Serious | Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels. |
| Critical | Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks. |
| Urgent | Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. |

### Potential Vulnerabilities

# WAS Scan Report

Potential Vulnerabilities indicate that the scanner observed a weakness or error that is commonly used to attack a web application, and the scanner was unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following-up with manual analysis. For example, the exploitability of a QID may be influenced by characteristics that the scanner cannot confirm, such as the web application's network architecture, or the test to confirm exploitability requires more intrusive testing than the scanner is designed to conduct.

| | |
|---|---|
| Minimal | **Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.** |
| Medium | **Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.** |
| Serious | **Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.** |
| Critical | **Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.** |
| Urgent | **Presence of this vulnerability might enable intruders to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. For example in this scenario, the web application users can potentially be targeted if the application is exploited.** |

## Sensitive Content

Sensitive content may be detected based on known patterns (credit card numbers, social security numbers) or custom patterns (strings, regular expressions), depending on the option profile used. Intruders may gain access to sensitive content that could result in misuse or other exploits.

| | |
|---|---|
| Minimal | **Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.** |
| Medium | **Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.** |
| Serious | **Sensitive content was found in the web server response - a valid social security number or credit card information. This infomation disclosure could result in a confidentiality breach, and it gives intruders access to valid sensitive content that could be misused.** |

## Information Gathered

Information Gathered issues (QIDs) include visible information about the web application's platform, code, or architecture. It may also include information about users of the web application.



| | |
|---|---|
| Minimal | **Intruders may be able to retrieve sensitive information related to the web application platform.** |
| Medium | **Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.** |
| Serious | **Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.** |